Cyberint
A Check Point Company

Infinity External Risk Management Services

THREAT HUNTING USER DATASHEET

YOU DESERVE THE BEST SECURITY

Infinity External Risk Management's Threat Hunting User license provides a suite of product modules to support the research, investigation, and hunting of cyber threats. These capabilities help you to proactively defend against probable threats, investigate incidents after an attack is detected, and uncover hidden threats that bypassed existing security controls.

CHALLENGE

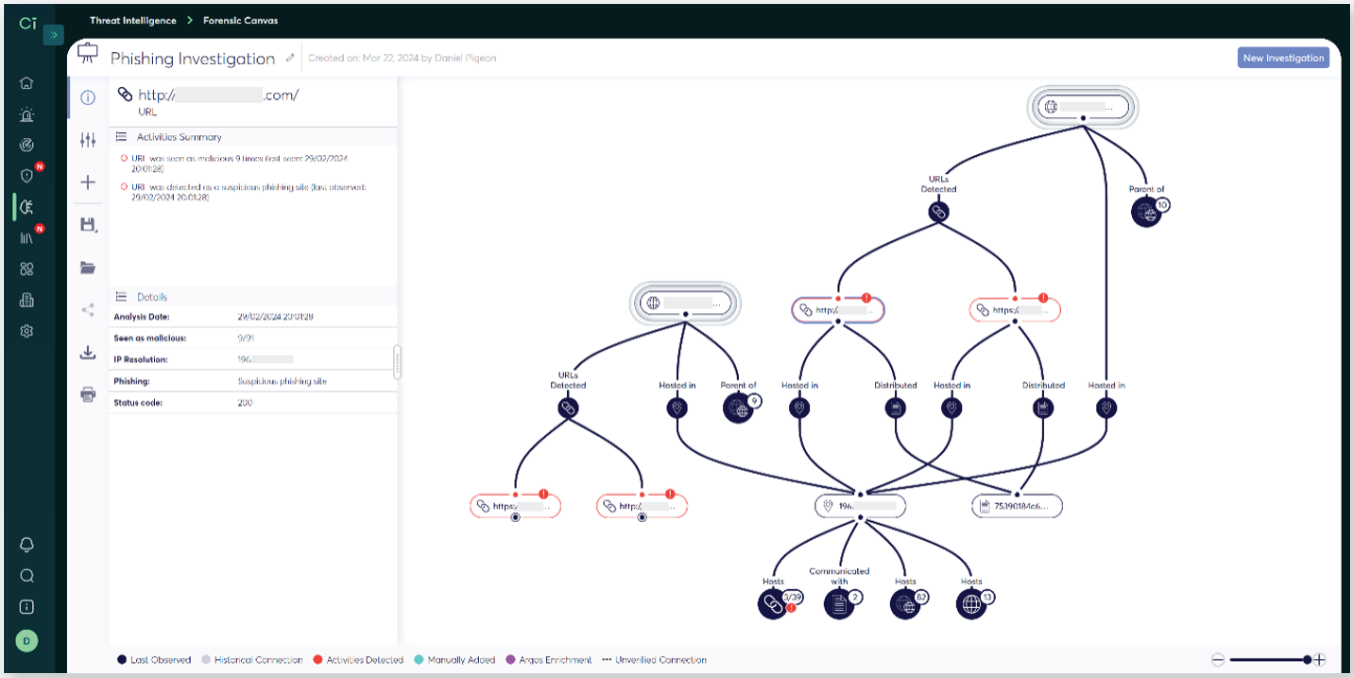
Many organizations seek to elevate their cyber threat intelligence program but lack the insights needed to do so. While IoC feeds and broad-scope threat reports are valuable, they aren't tailored to the defender's organization. Advanced CTI teams need access to relevant data to understand their specific threat landscape, conduct deep-dive investigations, and proactively hunt for threats that existing security controls may have missed.

SOLUTION

Infinity ERM Threat Hunting Users get access to enhanced CTI capabilities along 3 dimensions: research, investigations, and threat hunting. Research capabilities shed light on the specific threats you're most likely to face. Investigations tools help you understand the full scope of an attack after it's been detected. Threat hunting activities are supported with the strategic intelligence and enriched IoCs you need to develop a hypothesis, conduct the hunt, and root our previously undetected threats.

KEY BENEFITS

- Level up your CTI program to increase its impact, reduce risk and demonstrate value.
- Research your regional and industry-specific threat landscape to understand the risks you face.
- Run thorough investigations to uncover the full extent of the malicious infrastructure targeting you.
- Gain visibility into the deep and dark web and run complex search queries through the Infinity ERM Intel Data Lake.
- Develop accurate threat hunting hypotheses and access the data you need to uncover hidden threats.



http:/[redacted].com/
URL

Activities Summary

- URL was seen as malicious 9 times (last seen: 29/02/2024 20:01:28)
- URL was detected as a suspicious phishing site (last observed: 29/02/2024 20:01:28)

Details

Analysis Date:	29/02/2024 20:01:28
Seen as malicious:	9/91
IP Resolution:	196.[redacted]
Phishing:	Suspicious phishing site
Status code:	200

Research Your Threat Landscape

The cyber threat landscape varies across regions and from one industry to the next. It is also in a constant state of evolution, as cybercriminals adopt new tools and methods. .

View Your Regional & Sectoral Landscape

Filter by region or country plus industry to see the threat groups most active in your organization's specific threat landscape.

Access A Threat Intel Knowledgebase

Infinity ERM's Threat Knowledgebase provides a wealth of data on threat actors, malware, and CVEs.

Monitor Threats On The Dark Web

Track and monitor specific threat actors, forums, and marketplaces with the Intel Data Lake module.

Conduct Forensic Investigations

Once an attack has been detected, it's essential to quickly uncover the extent of the malicious activity so the risks can be fully mitigated.

Investigate Malicious Infrastructure

Enter a malicious IoC to launch an investigation and uncover additional malicious infrastructure.

Leverage A Dark Web Search Engine

Infinity ERM's Intel Data Lake supports complex queries, providing exclusive insights into the deep and dark web.

Establish An Early Warning System

Run complex queries, save them as custom alerting rules, and receive notifications in real-time when there's a hit.

Proactively Hunt For Undetected Threats

Threat Hunting programs identify threats that have bypassed existing security controls. Infinity ERM provides deep insights and IoC data to support these activities.

View Your Landscape's Common TTPs

Understand the most common TTPs used by the bad actors in your landscape.

Craft A Threat Huning Hypothesis

Develop a hypothesis that will increase the chances of a successful hunt.

Access & Download Enriched IoC Data

Access enriched IoC data associated with the specific threats you would like to hunt for.

> **Because we're a small team, the Check Point analysts are like an extension of us, which really helps from a risk management standpoint.**
>
> Evans Duvall, Cyber Security Engineer, Terex

> **We realized that Check Point was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.**
>
> Benjamin Bachmann, Head of Group Information Security, Ströer

> **Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Check Point to help us automatically detect and takedown these threats.**
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies

SCHEDULE A DEMO

Recognition As An Industry Leader From Trusted Analysts

Gartner | FROST & SULLIVAN | G2 | IDC

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm